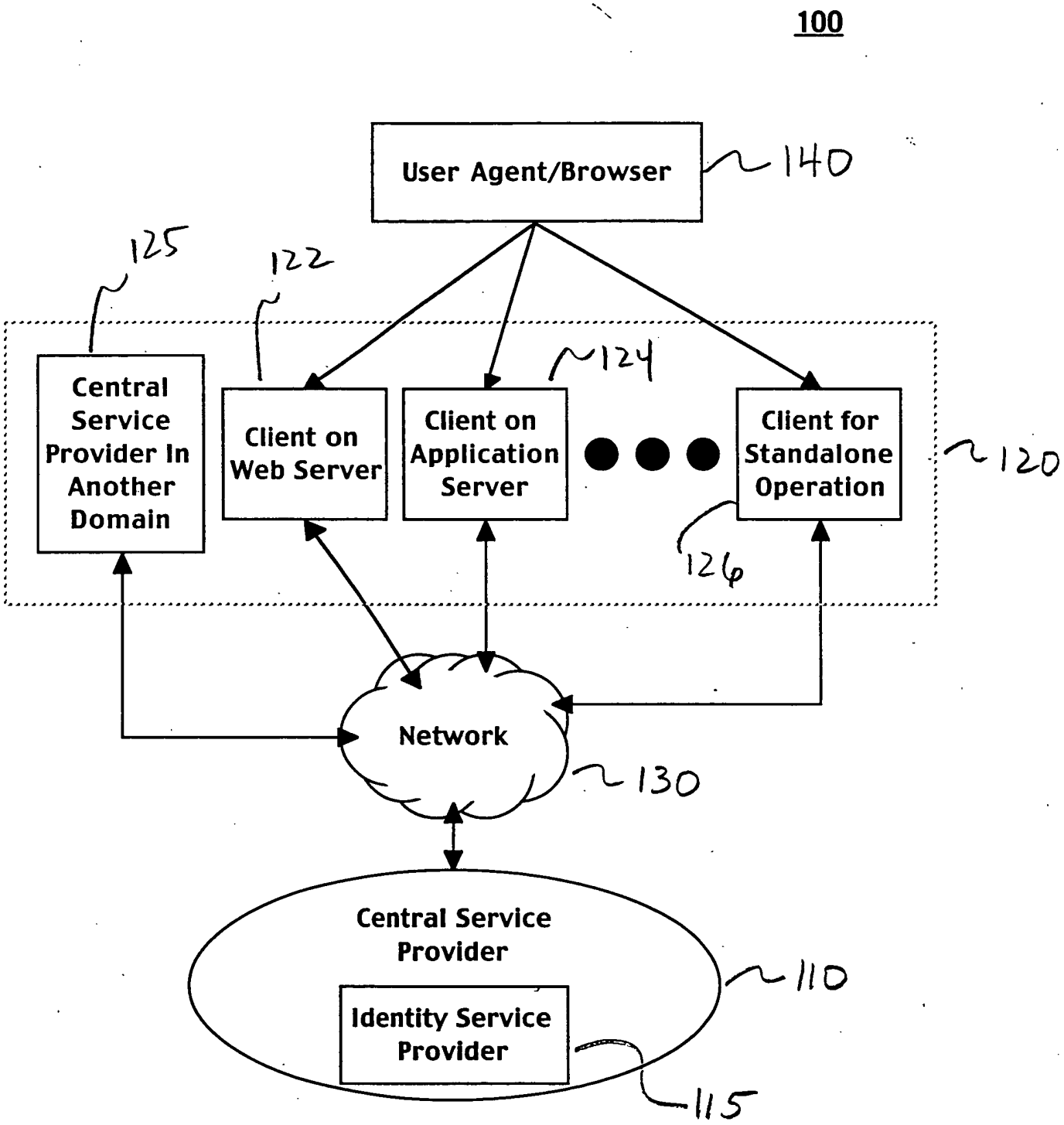
100
User Agent/Browser
140
125
122
124
Central Service Provider In Another Domain
Client on Web Server
Client on Application Server
Client for Standalone Operation
120
126
Network
130
Central Service Provider
110
Identity Service Provider
115

Fig. 1

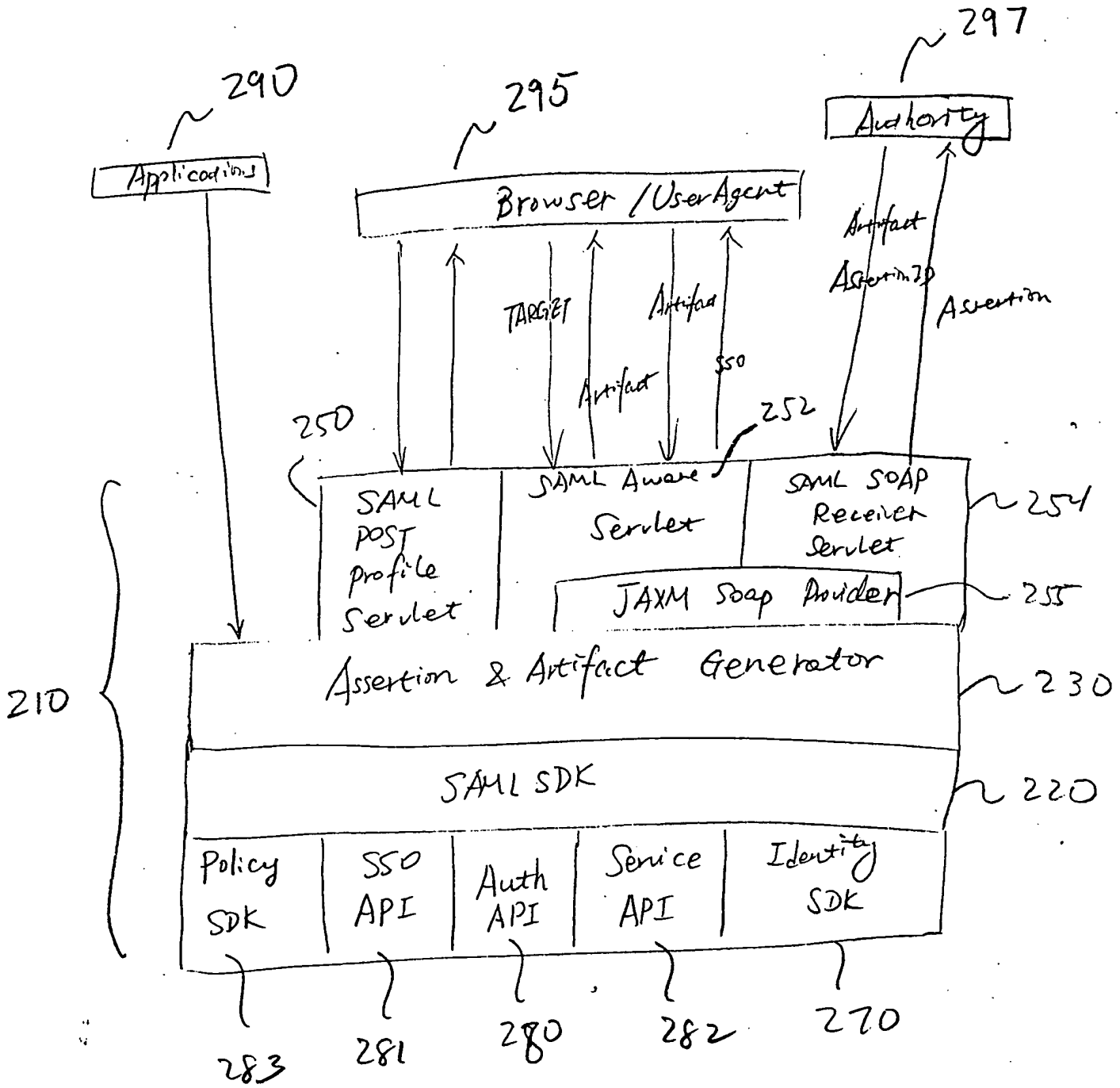
297
290
295
Authority
Application
Browser / UserAgent
Artifact
Assertion
TARGET
Artifact
Artifact
SSO
Assertion
250
252
SAML POST profile Servlet
SAML Aware Servlet
SAML SOAP Receiver Servlet
254
JAXM Soap Provider
255
210
Assertion & Artifact Generator
230
SAML SDK
220
Policy SDK
SSO API
Auth API
Service API
Identity SDK
283
281
280
282
270

Fig. 2

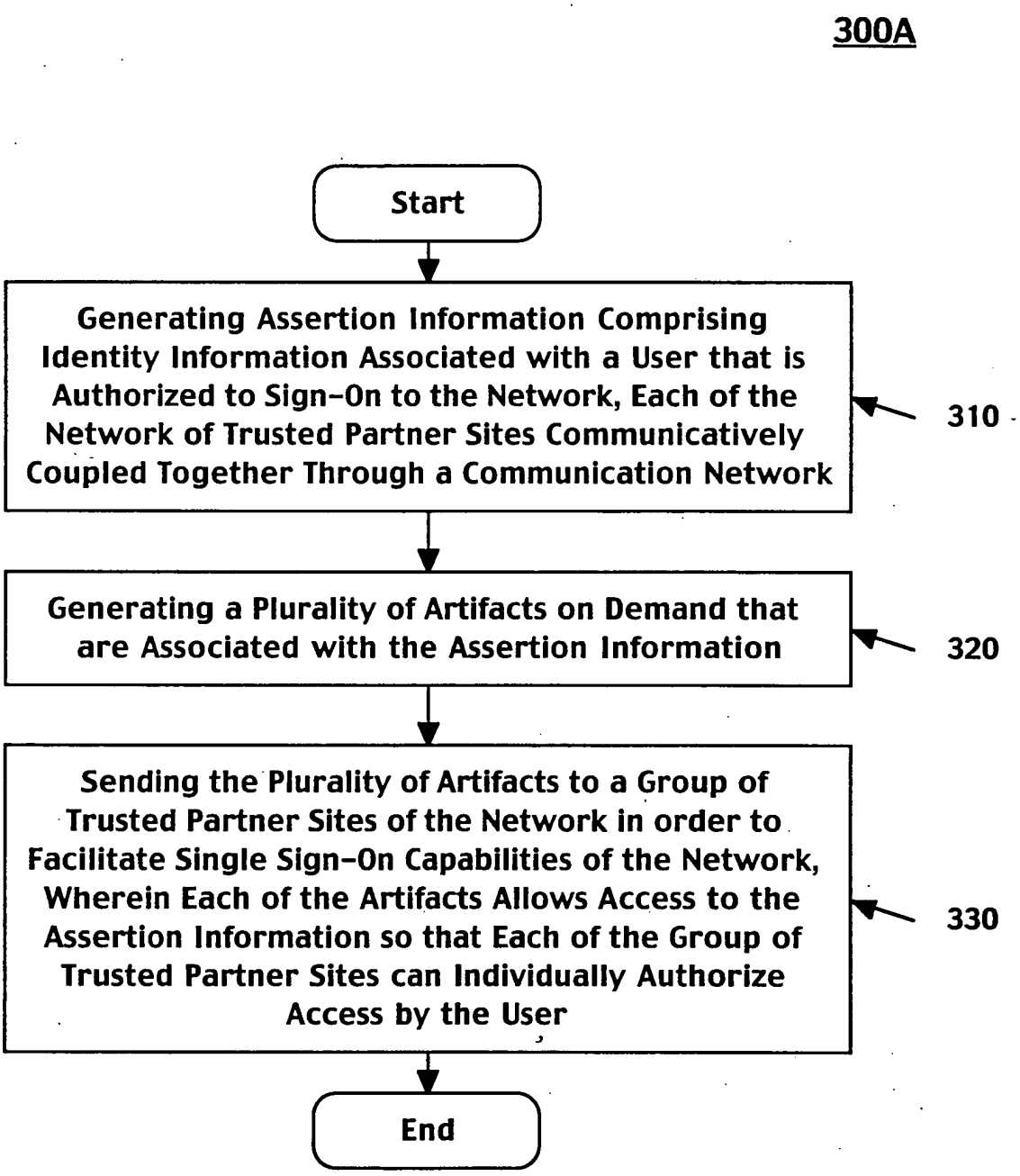
300A
Start
Generating Assertion Information Comprising Identity Information Associated with a User that is Authorized to Sign-On to the Network, Each of the Network of Trusted Partner Sites Communicatively Coupled Together Through a Communication Network
310
Generating a Plurality of Artifacts on Demand that are Associated with the Assertion Information
320
Sending the Plurality of Artifacts to a Group of Trusted Partner Sites of the Network in order to Facilitate Single Sign-On Capabilities of the Network, Wherein Each of the Artifacts Allows Access to the Assertion Information so that Each of the Group of Trusted Partner Sites can Individually Authorize Access by the User
330
End

Fig. 3A

300B

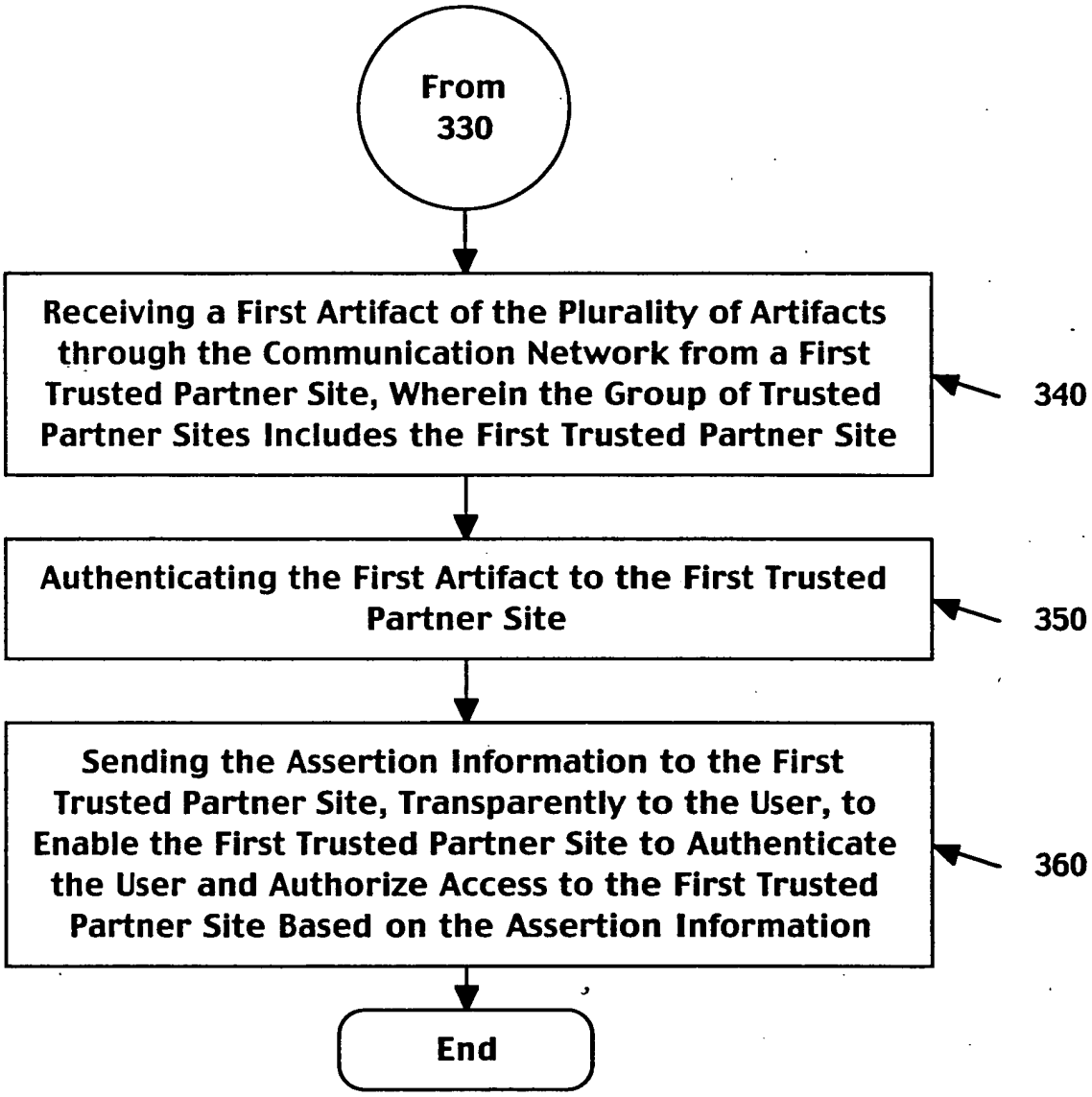
From 330
Receiving a First Artifact of the Plurality of Artifacts through the Communication Network from a First Trusted Partner Site, Wherein the Group of Trusted Partner Sites Includes the First Trusted Partner Site
340
Authenticating the First Artifact to the First Trusted Partner Site
350
Sending the Assertion Information to the First Trusted Partner Site, Transparently to the User, to Enable the First Trusted Partner Site to Authenticate the User and Authorize Access to the First Trusted Partner Site Based on the Assertion Information
360
End

Fig. 3B

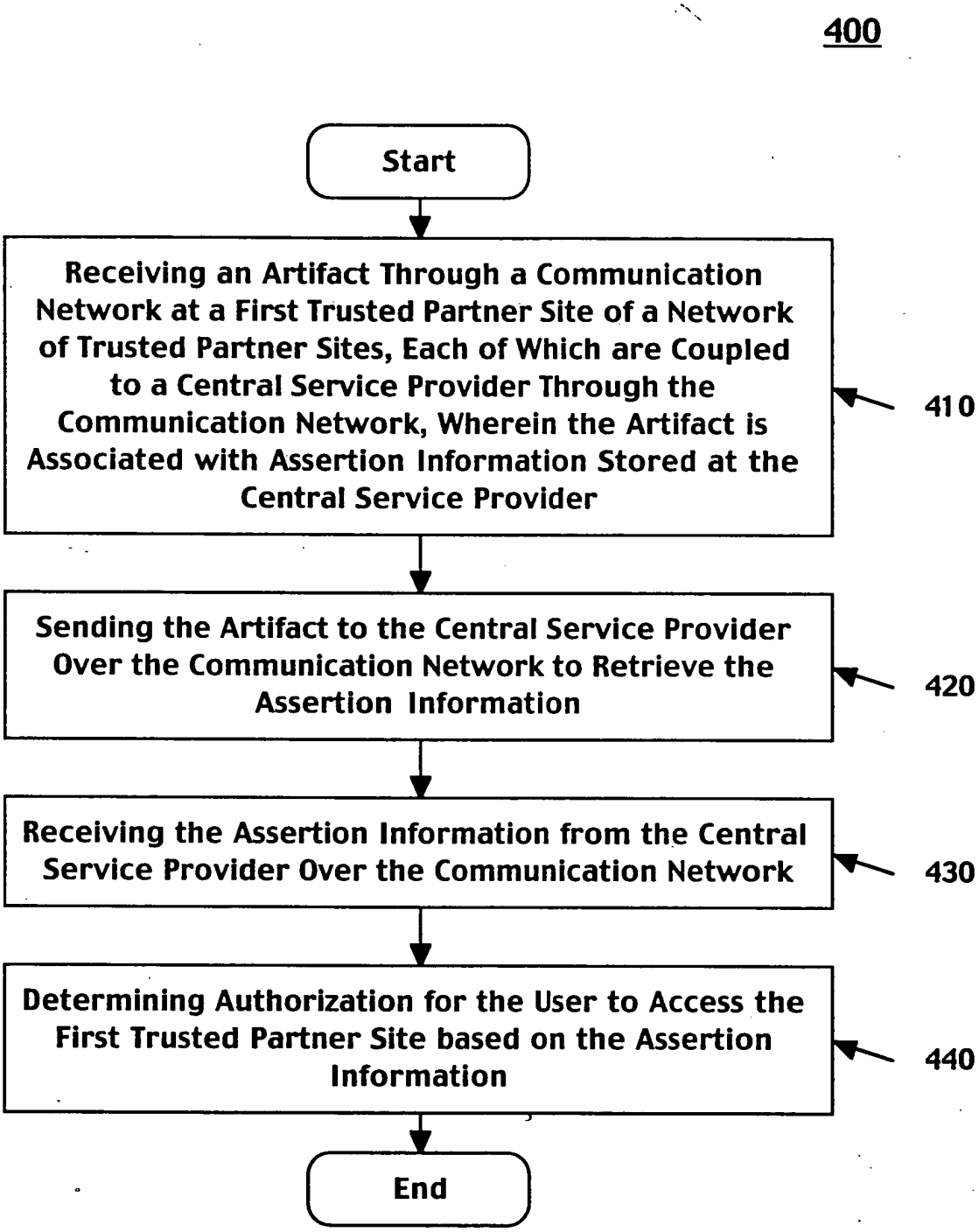
400
Start
Receiving an Artifact Through a Communication Network at a First Trusted Partner Site of a Network of Trusted Partner Sites, Each of Which are Coupled to a Central Service Provider Through the Communication Network, Wherein the Artifact is Associated with Assertion Information Stored at the Central Service Provider
410
Sending the Artifact to the Central Service Provider Over the Communication Network to Retrieve the Assertion Information
420
Receiving the Assertion Information from the Central Service Provider Over the Communication Network
430
Determining Authorization for the User to Access the First Trusted Partner Site based on the Assertion Information
440
End

Fig. 4

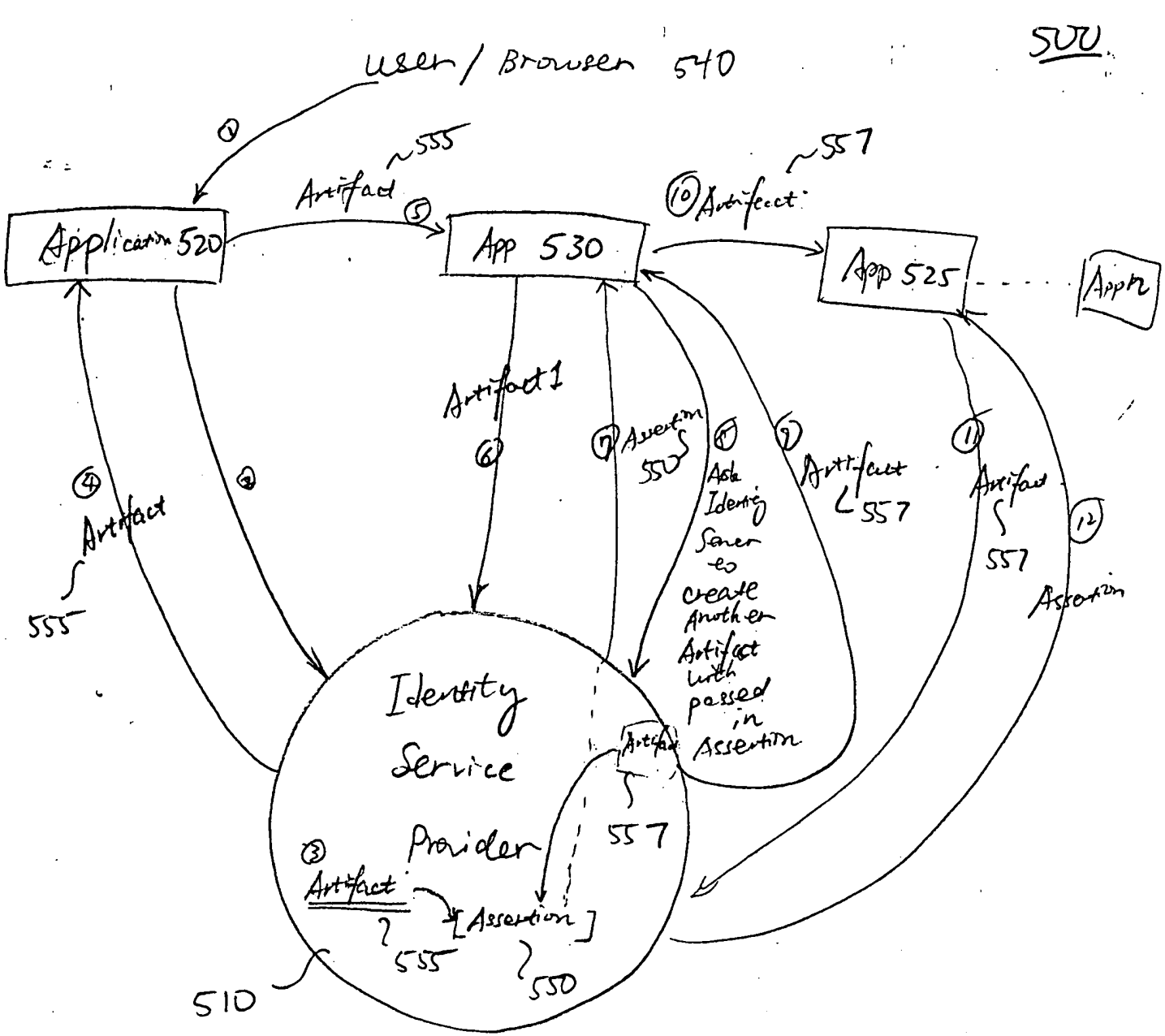
500
User / Browser 540
Application 520
App 530
App 525
Appn
Artifact
555
557
Assertion
550
Artifact 1
Ask Identity Server to create Another Artifact with passed in Assertion
Identity Service Provider
[Assertion]
510

Fig. 5

600

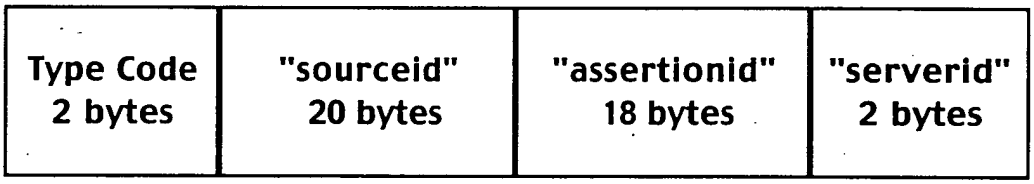
Type Code
2 bytes
"sourceid"
20 bytes
"assertionid"
18 bytes
"serverid"
2 bytes

Fig. 6

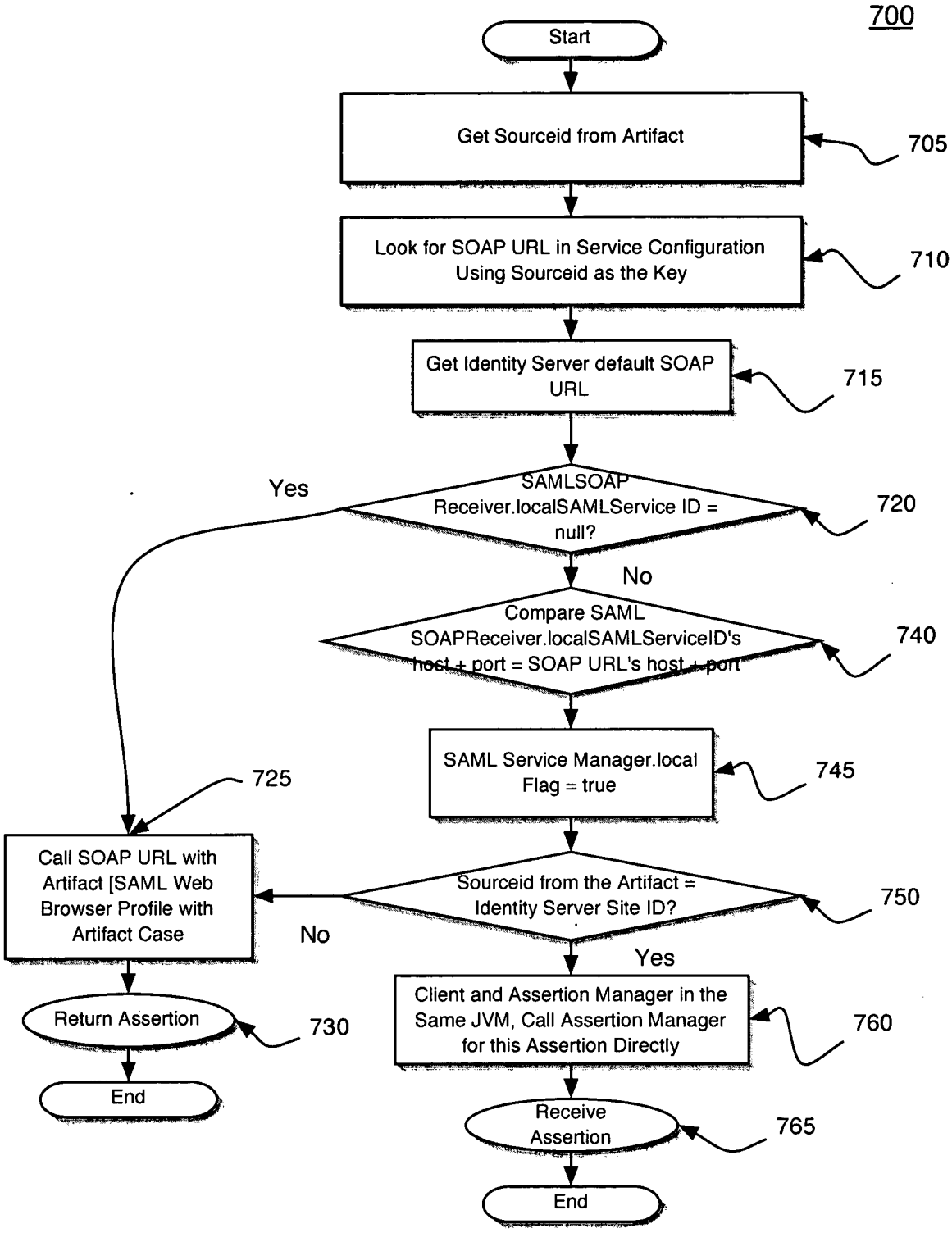
700
Start
Get Sourceid from Artifact
705
Look for SOAP URL in Service Configuration Using Sourceid as the Key
710
Get Identity Server default SOAP URL
715
SAMLSOAP Receiver.localSAMLService ID = null?
720
Yes
No
Compare SAML SOAPReceiver.localSAMLServiceID's host + port = SOAP URL's host + port
740
SAML Service Manager.local Flag = true
745
725
Call SOAP URL with Artifact [SAML Web Browser Profile with Artifact Case
Sourceid from the Artifact = Identity Server Site ID?
750
No
Yes
Return Assertion
730
Client and Assertion Manager in the Same JVM, Call Assertion Manager for this Assertion Directly
760
End
Receive Assertion
765
End

Fig. 7